JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Shielding in IoT Network of a Warehouse

[1]**Prof.Leena Patil,** [2]**Mohit Patil Author,** [3]**Niraj Chalke,**[4]**Aditya Walmiki,**[5]**Harsh Sawant**

[1]Professor, [2]Student, [3]Student,[4]Student,[5]Student
Dept. of Electronics & Telecommunication
Xavier Institute of Engineering ,Mumbai, India

Abstract : IoT data shielding is a thorough strategy to protect IoT-related data that is stored in the systems. Warehouses are being rapidly transformed by the Internet of Things (IoT), which is opening up new possibilities for productivity and efficiency. IoT networks, however, are also susceptible to a range of security risks, including denial-of-service attacks, illegal access, and data theft. This research leverages cloud computing to provide a data shielding architecture for IoT networks in warehouses. The framework shields data against unwanted access and use by combining a number of security measures, such as access control, and encryption. The creation of a data shielding framework that can assist in defending IoT networks in warehouses against security risks is the main objective of this project. It will be possible for businesses to gain from this.

IndexTerms **- IoT, cloud computing, data shielding, security methods, and warehouse introduction**

I.INTRODUCTION

The explosive growth of the Internet of Things (IoT) has ushered in a new era of data-driven decision-making. Sensor nodes embedded in our environment generate a constant stream of valuable information, fuelling applications across diverse domains. Centralizing this data in data warehouses unlocks immense potential for analysis and knowledge extraction. However, with this power comes a critical responsibility: safeguarding the privacy and security of this sensitive data. Personal information from smart homes, critical infrastructure data, and sensitive financial transactions collected by IoT sensors demand robust protection against unauthorized access and malicious exploitation.

Traditionally, data privacy in IoT networks has relied on techniques like anonymization and pseudonymization. However, these methods often come at the expense of data utility, hindering the ability to extract meaningful insights. Homomorphic encryption (HE) emerges as a powerful alternative, enabling computations on encrypted data without decryption, preserving data privacy while unlocking analytical power.

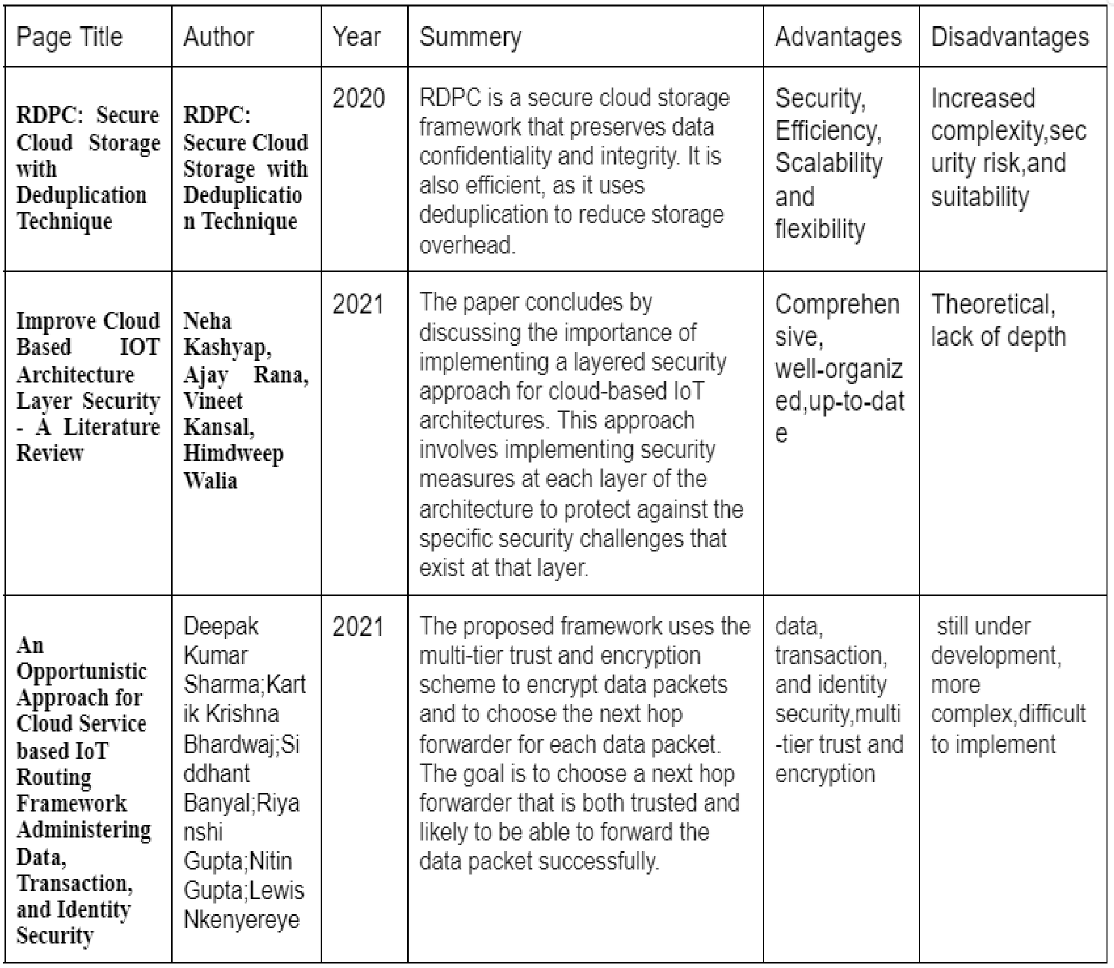
This research builds upon the promise of HE to develop a novel data shielding technique for IoT networks, ensuring data privacy and security throughout the data lifecycle, from sensor data collection to analysis within the data warehouse.

II. OBJECTIVES

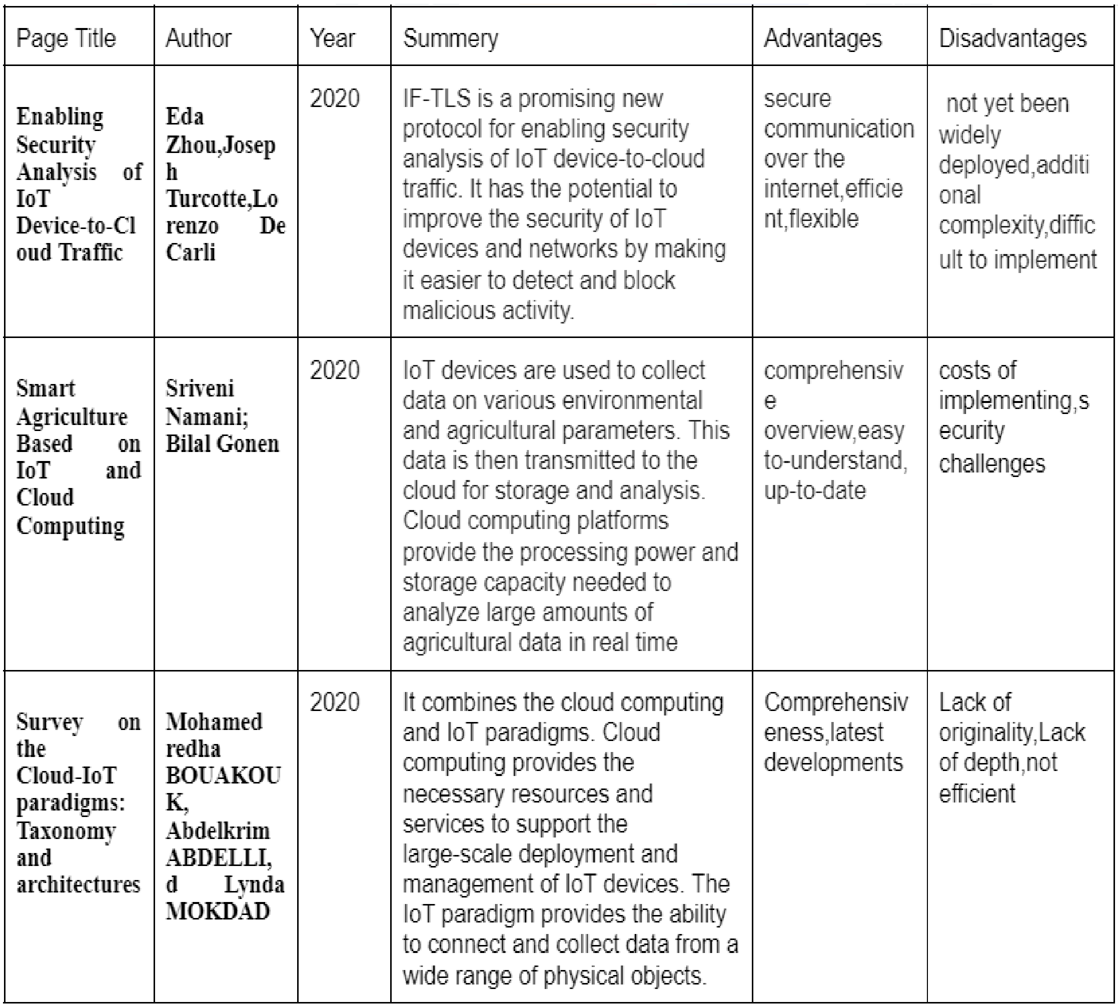
The objective is to develop a data shielding solution for the data of IoT devices in a IoT network of a Warehouse. This solution will protect sensitive data from malicious attacks and ensure the privacy and security of the data.The system is designed to be scalable and flexible, so that it can be used in a variety of warehouses. It will also be designed to be easy to use and maintain.To Implement Transparent Transactions

III. LITERATURE REVIEW

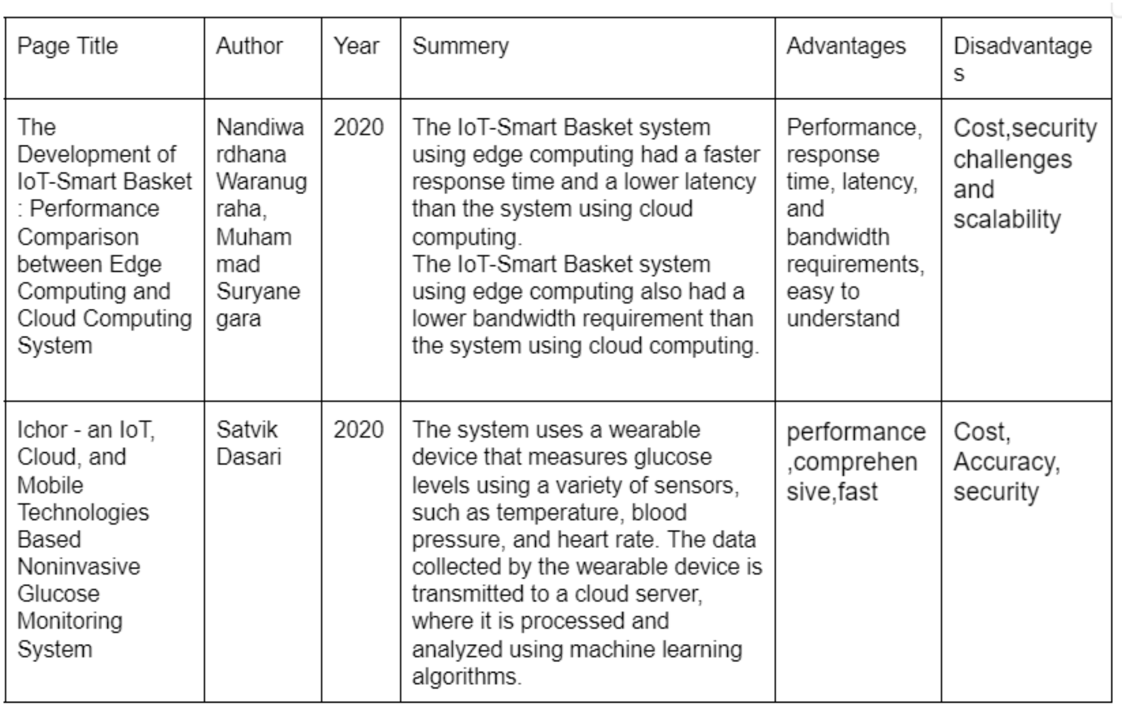
In conducting the literature review for our project, we delved into several IEEE papers to acquire a comprehensive understanding of the current state-of-the-art in the relevant field. These IEEE publications served as invaluable resources, offering insights into key methodologies, technological advancements, and theoretical frameworks that informed and guided the development of our project. By synthesizing information from these rigorously peer-reviewed sources, we aimed to ensure the robustness and validity of our approach, aligning our work with established research and fostering a foundation of knowledge that enhances the credibility and innovation of our project. The wealth of knowledge gleaned from these IEEE papers not only facilitated a nuanced comprehension of the existing literature but also inspired creative solutions and methodologies, positioning our project within the broader context of cutting-edge research in the field.



Page Title	Author	Year	Summery	Advantages	Disadvantages
RDPC: Secure Cloud Storage with Deduplication Technique	**RDPC: Secure Cloud Storage with Deduplication Technique**	2020	RDPC is a secure cloud storage framework that preserves data confidentiality and integrity. It is also efficient, as it uses deduplication to reduce storage overhead.	Security, Efficiency, Scalability and flexibility	Increased complexity,security risk,and suitability
Improve Cloud Based IOT Architecture Layer Security - A Literature Review	**Neha Kashyap, Ajay Rana, Vineet Kansal, Himdweep Walia**	2021	The paper concludes by discussing the importance of implementing a layered security approach for cloud-based IoT architectures. This approach involves implementing security measures at each layer of the architecture to protect against the specific security challenges that exist at that layer.	Comprehensive, well-organized,up-to-date	Theoretical, lack of depth
An Opportunistic Approach for Cloud Service based IoT Routing Framework Administering Data, Transaction, and Identity Security	Deepak Kumar Sharma;Kartik Krishna Bhardwaj;Siddhant Banyal;Riyanshi Gupta;Nitin Gupta;Lewis Nkenyereye	2021	The proposed framework uses the multi-tier trust and encryption scheme to encrypt data packets and to choose the next hop forwarder for each data packet. The goal is to choose a next hop forwarder that is both trusted and likely to be able to forward the data packet successfully.	data, transaction, and identity security,multi-tier trust and encryption	still under development, more complex,difficult to implement



Page Title	Author	Year	Summery	Advantages	Disadvantages
Enabling Security Analysis of IoT Device-to-Cloud Traffic	**Eda Zhou,Joseph Turcotte,Lorenzo De Carli**	2020	IF-TLS is a promising new protocol for enabling security analysis of IoT device-to-cloud traffic. It has the potential to improve the security of IoT devices and networks by making it easier to detect and block malicious activity.	secure communication over the internet,efficient,flexible	not yet been widely deployed,additional complexity,difficult to implement
Smart Agriculture Based on IoT and Cloud Computing	**Sriveni Namani; Bilal Gonen**	2020	IoT devices are used to collect data on various environmental and agricultural parameters. This data is then transmitted to the cloud for storage and analysis. Cloud computing platforms provide the processing power and storage capacity needed to analyze large amounts of agricultural data in real time	comprehensive overview,easy to-understand, up-to-date	costs of implementing,security challenges
Survey on the Cloud-IoT paradigms: Taxonomy and architectures	**Mohamed redha BOUAKOUK, Abdelkrim ABDELLI, d Lynda MOKDAD**	2020	It combines the cloud computing and IoT paradigms. Cloud computing provides the necessary resources and services to support the large-scale deployment and management of IoT devices. The IoT paradigm provides the ability to connect and collect data from a wide range of physical objects.	Comprehensiveness,latest developments	Lack of originality,Lack of depth,not efficient



Page Title	Author	Year	Summery	Advantages	Disadvantages
The Development of IoT-Smart Basket : Performance Comparison between Edge Computing and Cloud Computing System	Nandiwardhana Waranugraha, Muhammad Suryanegara	2020	The IoT-Smart Basket system using edge computing had a faster response time and a lower latency than the system using cloud computing. The IoT-Smart Basket system using edge computing also had a lower bandwidth requirement than the system using cloud computing.	Performance, response time, latency, and bandwidth requirements, easy to understand	Cost,security challenges and scalability
Ichor - an IoT, Cloud, and Mobile Technologies Based Noninvasive Glucose Monitoring System	Satvik Dasari	2020	The system uses a wearable device that measures glucose levels using a variety of sensors, such as temperature, blood pressure, and heart rate. The data collected by the wearable device is transmitted to a cloud server, where it is processed and analyzed using machine learning algorithms.	performance ,comprehensive,fast	Cost, Accuracy, security

IV. Limitations of Existing system

Existing data shielding systems for IoT networks in warehouses often have limitations in terms of scalability, performance, security, and ease of use.

A. Scalability:
Many existing systems are not designed to scale to large networks of IoT devices, which can make them difficult to deploy and manage in a large warehouse environment.

B. Performance:
Some existing systems impose a significant performance overhead on IoT devices, which can reduce their efficiency and impact the overall performance of the warehouse
network.

C. Security:
Some existing systems have security vulnerabilities that can be exploited by
attackers, putting the data in the warehouse network at risk.

D. Ease of use:
Many existing systems are complex to configure and manage, which can
make it difficult for businesses to implement and maintain them effectively.

V. Problem Statement

"To mitigate the security risks and performance limitations of traditional data transfer methods in IoT networks, Cloud Computing Technology can be used to provide a more secure, reliable, and scalable data transfer solution as it offers a variety of security features for protecting the data from unauthorized access, manipulation or destruction."

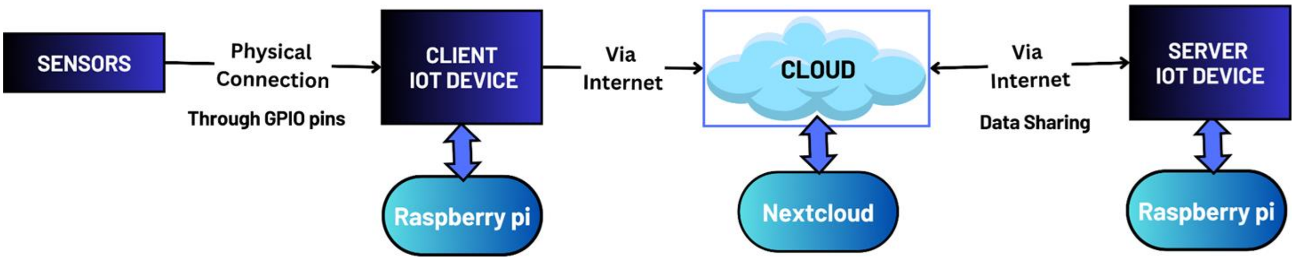
I. RESEARCH METHODOLOGY

The methodology section outline the plan and method that how the study is conducted. This includes Data and Sources of Data, study’s variables and analytical framework. The detailsare as follows;

3.1Framework:

To Protect or Disguise the Information Obtained from IoT Devices in the IoT Network of Using lightweight warehousing system techniques, we will concentrate on resource-constrained environment security optimization. The first step is to build an IoT network infrastructure that is a duplicate of the network found in current systems.

To extract the data from the surroundings and environment, many sensors are used. Temperature and proximity sensors are the sensors that are utilized to extract the surrounding data. With the aid of the ESP module, the collected data is subsequently moved to the Raspberry Pi, where it is thereafter stored until it is needed on the Cloud server. Here, we're using Next Cloud, an installed cloud server on a Raspberry Pi. Additionally, the disparate Cloud-based methods are used to secure the IoT data extraction.



3.2 HARDWARE Used

A. Raspberry Pi

A Raspberry Pi is a small, low-cost computer that can be used for a variety of purposes. We are using it as a central unit for an IoT network. In an IoT network, the Raspberry Pi can be used to collect data from multiple sensors and send that data to the cloud To act as the central unit for an IoT network, the Raspberry Pi would need to be connected to the sensors and to the internet. The Raspberry Pi would then use software to collect the data from the sensors and send it to the cloud.

B. Temperature Sensor:

Devices that measure an object's or environment's temperature are called temperature sensors. They are essential parts of applications where precise temperature control is necessary. The NTC Thermistor Temperature Sensor Module 3 Pin uses a thermistor sensor to detect temperature and is a low-cost, compact module. It is sensitive to the temperature of the surrounding environment. It reacts strongly to changes in temperature. Generally speaking, it is employed to measure the ambient temperature. It is possible to alter the temperature detecting threshold by adjusting the potentiometer.

C. Motion Sensors:

A warehouse network can improve security, automate lighting management, and increase energy efficiency by integrating a PIR (Passive Infrared) motion sensor. PIR motion sensors track variations in infrared light resulting from moving objects, including humans.

3.3 SOFTWARE Used

A. NextCloud

It is an application for a cloud server that lets you store and distribute Internet of Things data online. Since it is a self-hosted solution, you are in total control of your data. Because it is scalable, secure, and has many characteristics that are beneficial for IoT networks, Nextcloud is a solid option for IoT networks. We store and exchange data from IoT devices and their sensors using Nextcloud. Additionally, we might use Nextcloud to work together with other users on projects like making dashboards to display your IoT data or creating new IoT apps.

B. Maria DB

MariaDB is a fork of the relational database management system (RDBMS) MySQL that is developed by the community and sponsored by businesses. Under the terms of the GNU General Public License, it is meant to stay free and open-source software (GPL). MariaDB, the daughter of MySQL's original developer Michael Widenius, is the inspiration behind the name MariaDB.

C. Dietpi OS

DietPi is a lightweight Linux operating system (OS) distribution designed for the Raspberry Pi and other single-board computers (SBCs). It is based on Debian and is known for its ease of use, performance, and security.

D. Rpi OS

Raspberry Pi OS is a Linux operating system (OS) distribution based on Debian specifically designed for the Raspberry Pi and other single-board computers (SBCs). It is a general-purpose OS that can be used for a variety of tasks

IV. RESULTS AND DISCUSSION

Here are the results of our first implementation for our project "Data Shielding in IoT Network of a Warehouse " For the first phase of our project we successfully installed and configured Nextcloud as our Personal self-hosted cloud as a Server on a Raspberry Pi.

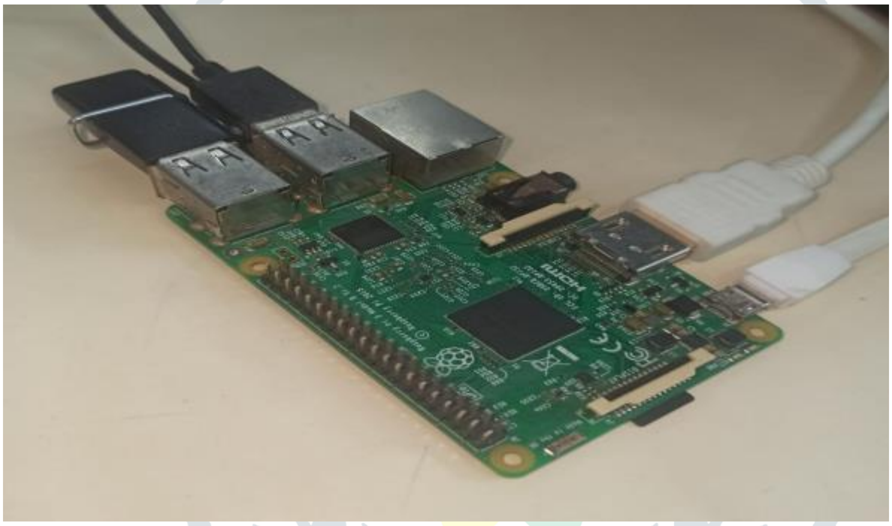
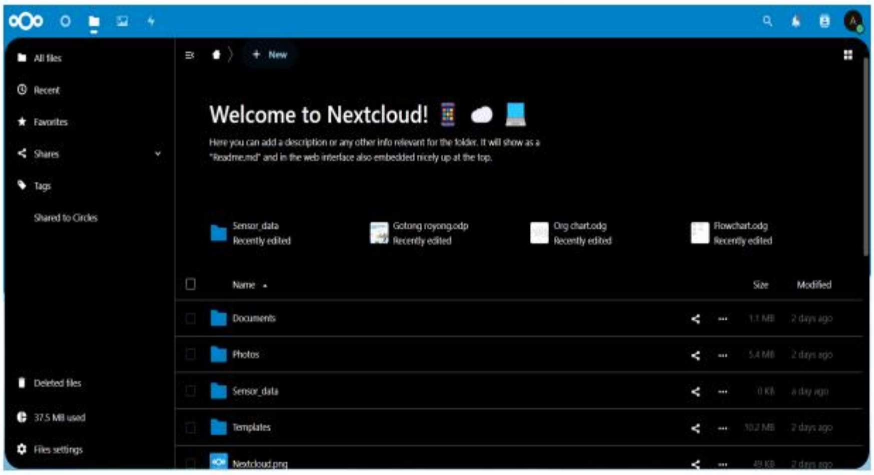


Fig 10.1 Result 1



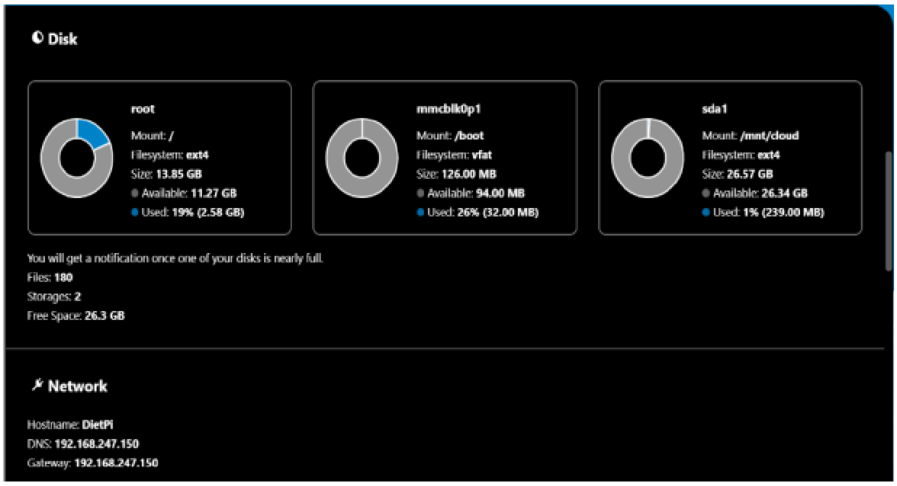
Welcome to Nextcloud!

Here you can add a description or any other info relevant for the folder. It will show as a "Readme.md" and in the web interface also embedded nicely up at the top.

Sensor_data Recently edited
Gotong royong.odp Recently edited
Org chart.odg Recently edited
Flowchart.odg Recently edited

Name	Size	Modified
Documents	1.1 MB	2 days ago
Photos	5.4 MB	2 days ago
Sensor_data	0 KB	a day ago
Templates	10.2 MB	2 days ago
Nextcloud.png	49 KB	2 days ago

Fig.10.2 Result



Disk

root
Mount: /
Filesystem: ext4
Size: 13.85 GB
● Available: 11.27 GB
● Used: 19% (2.58 GB)

mmcblk0p1
Mount: /boot
Filesystem: vfat
Size: 126.00 MB
● Available: 94.00 MB
● Used: 26% (32.00 MB)

sda1
Mount: /mnt/cloud
Filesystem: ext4
Size: 26.57 GB
● Available: 26.34 GB
● Used: 1% (239.00 MB)

You will get a notification once one of your disks is nearly full.
Files: 180
Storages: 2
Free Space: 26.3 GB

Network

Hostname: DietPi
DNS: 192.168.247.150
Gateway: 192.168.247.150

Fig. 10.3 Result

VI. Conclusion and Future Scope

In this project we demonstrated the feasibility of using lightweight algorithms to secure data acquired from IoT devices in a warehousing system. The project began by creating an IoT network infrastructure that replicated the network used in a present-day warehousing system. Different sensors were used to extract data from the environment, including temperature sensors and proximity sensors. The acquired data was then transferred to a Raspberry Pi using an ESP module. The data was then stored from the Raspberry Pi to a NextCloud cloud server. Different techniques were used to secure the extracted IoT data on the cloud server. These techniques included encryption and anonymization. Data is jumbled up by encryption, making it unreadable without the encryption key

Future Work The project can be extended in a number of ways. For example, the project could be extended to include more IoT devices and sensors. The project could also be extended to include more sophisticated security techniques. Additionally, the project could be extended to test the security of the system in a real-world environment.

References

[1] R. Patil Rashmi; Yatin Gandhi; Vinaya Sarmalkar; Prajakta Pund; Vinit Khetani “RDPC: Secure Cloud Storage with Deduplication Technique” 2020 Fourth International Conference on I-SMAC, DOI: 10.1109/I-SMAC49090.2020.9243442

[2] Neha Kashyap, Ajay Rana, Vineet Kansal, Himdweep Walia “Improve Cloud Based IoT Architecture Layer Security - A Literature Review “2021 International Conference on Computing, DOI: 10.1109/ICCCIS51004.2021.9397146

[3] Deepak Kumar Sharma;Kartik Krishna Bhardwaj;Siddhant Banyal;Riyanshi Gupta;Nitin Gupta;Lewis Nkenyereye “An Opportunistic Approach for Cloud Service based IoT Routing Framework Administering Data, Transaction, and Identity Security” IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2021.3078810

[4] Eda Zhou,Joseph Turcotte,Lorenzo De Carli“Enabling Security Analysis of IoT Device-to-Cloud Traffic ” , 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), DOI 10.1109/TrustCom50675.2020.00258

[5] Sriveni Namani; Bilal Gonen “Smart Agriculture Based on IoT and Cloud Computing”, 2020 3rd International Conference on Information and Computer Technologies (ICICT), DOI: 10.1109/ICICT50521.2020.00094 .

[6] Mohamed redha BOUAKOUK, Abdelkrim ABDELLI, d Lynda MOKDAD, “Survey on the Cloud-IoT paradigms: Taxonomy and architectures” 2020 IEEE Symposium on Computers and Communications (ISCC), DOI: 10.1109/ISCC50000.2020.9219638

[7] Nandiwardhana Wara Nugraha, Muhammad Suryanegara, “The Development of IoT-Smart Basket : Performance Comparison between Edge Computing and Cloud Computing System ” 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE), DOI: 10.1109/IC2IE50715.2020.9274596

[8] Satvik Dasari , “Ichor - an IoT, Cloud, and Mobile Technologies Based Noninvasive Glucose Monitoring System ” 2020 IEEE International IOT, Electronics and Mechatronics Conference (AIMTRONICS), DOI: 10.1109/IEMTRONICS51293.2020.921634

[9] XIANG LI1, QIXU WANG2,”Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach”2019 ,DOI:10.1109/ACCESS.2018.2890432

[10] Muhammad Kazim, Lu Liu"A Framework for Orchestrating Secure and Dynamic Access of IoT Services in Multi-Cloud Environments”2018,DOI:10.1109/ACCESS.2018.2873812

[11] IHSAN ALI “ Data Collection in Studies on Internet ofThings (IoT), Wireless Sensor Networks(WSNs), and Sensor Cloud (SC):Similarities and Differences ” DOI:10.36227/techrxiv.14039486.v1

[12] Saad Mubeen,Sara Abbaspour Asadollah “Management of Service Level Agreements forCloud Services in IoT: A Systematic Mapping Study”DOI:10.1109/ACCESS.2017.2744677

[13] Ameer Pichan, Mihai Lazarescu, Sie Teng Soh et al, “A Logging Model for Enabling Digital Forensics in IoT, in an Inter-connected IoT, Cloud Ecosystems.” 2020,Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), DOI 978-1-7281-6823-4/20/$31.00

[14] Amr M.T. , Ali-Eldin “A CLOUD-BASED TRUST COMPUTING MODEL For The SOCIAL INTERNET OF THINGS” 2021,International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) , DOI 10.1109/MIUCC52538.2021.9447667

[15] Anuj Kumar, Vinod Jain, Anupam Yadav, “A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique”2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC) IEEE, DOI: 10.1109/PARC49193.2020.236666

[16] Daniel D-az López ,1Mar-aBlancoUribe,1Claudia Santiago Cely ,1Andrés Vega Torres “Shielding IoT against cyber-attacks: An event-based approach using SIEM”2018Wireless Communications and Mobile Computing 2018(Security, Privacy, and Trust on Internet of Things) DOI:10.1155/2018/3029638

[17] MA Ahad, G Tripathi, S Zafar, F Doja -”IoT data management—Security aspects of information linkage in IoT systems”2021 Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi 110062, India. DOI https://doi.org/10.1007/978-3-030-33596-0_18

[18] Halah Mohammed Al-Kadhim and Hamed S. Al-Raweshidy “Energy Efficient and Reliable Transport of Data in Cloud-Based IoT” DOI:10.1109/ACCESS.2019.2917387